



# Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 02 June 2005

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

## Daily Highlights

- The Dover Post reports Delaware State University has installed security measures on its Website after discovering someone hacked into it and the school's e-mail system in an attempt to steal identity information. (See item [4](#))
- The Greeley Tribune reports that Colorado State University is piloting a national animal identification system that will rely on grid-computing technology to process massive amounts of animal tracking data, which would be valuable should there be a disease outbreak. (See item [12](#))
- The Albuquerque Tribune reports New Mexico has devised a plan for a potential flu pandemic which includes getting the vaccines and protective equipment to state health care workers and shutting down public places such as schools and shopping malls. (See item [18](#))

### DHS/IAIP Update Fast Jump

**Production Industries:** [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

**Sustenance and Health:** [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS/IAIP Products & Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *June 01, Nuclear Regulatory Commission* — **Nuclear Regulatory Commission adds Syria to list of embargoed destinations.** The Nuclear Regulatory Commission (NRC) has revised its import/export regulations to reflect current U.S. law and foreign policy on Syria. The changes remove Syria from the list of restricted destinations for exports and add it to the list of

embargoed destinations. These changes are necessary to conform the NRC's export controls to the Syria Accountability and Lebanese Sovereignty Restoration Act of 2003. The regulations, published in the Federal Register on May 25, are contained in Title 10 of the Code of Federal Regulations, Part 110. They prohibit the export of nuclear material or equipment to Syria under a general license. A general license allows for the export of certain nuclear equipment and material without the filing of an application with the NRC. Potential shipments of nuclear material to Syria will now require the filing of an application requesting a specific license. Source: <http://www.nrc.gov/reading-rm/doc-collections/news/2005/05-086.html>

2. ***May 31, Pacific Gas and Electric* — Utility files final report on investigation into location of fuel segments.** Pacific Gas and Electric Company (PG&E) has provided the Nuclear Regulatory Commission (NRC) with a final report on the investigation into the location of segments of a used nuclear fuel rod at its Humboldt Bay Power Plant near Eureka, CA. The investigation began last June, when the utility reported to the NRC the discovery of conflicting records on the location of three, 18-inch long cut segments. These records indicate that the segments were either stored in the used fuel pool in 1968 or were shipped to a licensed nuclear waste facility in 1969. The final report to the NRC details the work that has been conducted over to determine the possible location of the segments and to rule out unlikely locations and scenarios. PG&E's investigation points to two reasonable possibilities regarding the location of the fuel segments: 1) they remain in the used fuel pool; or 2) they were shipped offsite to one of three licensed facilities. The investigation also found no evidence to support the possibility that the fuel segments were stolen from the facility.

Source: [http://www.pge.com/news/news\\_releases/q2\\_2005/050531.html](http://www.pge.com/news/news_releases/q2_2005/050531.html)

3. ***May 25, Midwest ISO* — Midwest Independent System Operator evaluation shows sufficient reserve margins for summer power demand.** Officials at the Midwest Independent System Operator (ISO) have issued a region-wide summer evaluation indicating the region has sufficient generation capacity to meet the expected summer peak power demand. According to the evaluation, the Midwest ISO will see an estimated peak of 114,479 MW. Available generation capacity is projected to be at 135,054 MW, providing a reserve margin of 18 percent. "We are confident that the generators in the Midwest ISO will be able to supply enough capacity to meet peak demand for the coming summer," said Midwest ISO president and CEO James P. Torgerson. The summer evaluation is an annual review that looks at the expected use of power compared to the amount of generation available to meet the needs of the footprint. The Midwest ISO considered the MAPP (Mid-Continent Area Power Pool), MAIN (Mid-America Interconnected Network) and ECAR (East Central Area Reliability Coordination Agreement) reliability regions' summer assessments. Reserve requirements are put into place as a precaution should power demands reach higher than anticipated levels or equipment is removed from service due to forced outages.

Source: [http://www.midwestmarket.org/publish/Document/2b8a32\\_103ef711180-7f210a48324a/2005-05-25%20prs%20rel%20-%20Midwest%20ISO%20Summer%20Release.pdf?action=download&property=Attachment](http://www.midwestmarket.org/publish/Document/2b8a32_103ef711180-7f210a48324a/2005-05-25%20prs%20rel%20-%20Midwest%20ISO%20Summer%20Release.pdf?action=download&property=Attachment)

[\[Return to top\]](#)

## **Chemical Industry and Hazardous Materials Sector**

Nothing to report.

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

Nothing to report.

[\[Return to top\]](#)

## **Banking and Finance Sector**

### **4. *June 01, Dover Post (DE)* — Hackers set up phishing scam from university Website.**

Delaware State University (DSU) installed security measures on its Website last week after discovering someone hacked into [www.desu.edu](http://www.desu.edu) and the school's e-mail system in an attempt to steal identity information. School information technology officials alerted the state police to the phishing scam on May 25. Hackers gained access to the DSU site and created a fake, hidden page that impersonated the site of an overseas bank, according to school spokesperson Carlos Holmes. Anyone who received a bogus e-mail from the scammer could have linked to the fake page and been asked for account information. At no time was any DSU student, academic, financial or administrative information stolen or at risk, Holmes said. The Delaware State Police High Tech Crimes Unit has launched an investigation that's currently ongoing.

Source: <http://www.doverpost.com/pages/newshackers.html>

### **5. *May 31, Associated Press* — Teens hack into school computer system for personal information.**

Police in Pennsylvania are investigating whether criminal charges are warranted after three teenagers allegedly broke into a Carlisle Area School District computer server and retrieved birth dates, addresses and Social Security numbers of employees and students.

"They're bright kids and they were able to navigate through the system. They kept trying things, and they're very persistent. They worked through it until they found a hole," said Mary Kay Durham, the school superintendent. The teens were caught after one told a classmate that he knew his Social Security number, and that student reported it to a teacher, Durham said.

Source: <http://www.poconorecord.com/local/rxf74117.htm>

[\[Return to top\]](#)

## **Transportation and Border Security Sector**

### **6. *June 01, Transportation Security Administration* — TSA begins third phase of Hazmat**

**Threat Assessment Program.** The Transportation Security Administration (TSA) began the third and final implementation phase of the Hazmat Threat Assessment Program this week with the fingerprinting of commercial truck drivers applying to renew or transfer the hazardous materials endorsement (HME) on their State-issued commercial drivers licenses. During phase one of the Hazmat Threat Assessment Program, TSA conducted name-based security threat assessments on all 2.7 million licensed hazardous materials (Hazmat) drivers to determine whether any presented a potential terrorist threat. Phase two augmented this effort by adding a fingerprint-based FBI criminal history records check and immigration status check for new HME applicants. This third and final phase will require drivers seeking to renew or transfer

their current HME to undergo the fingerprint-based security threat assessment. Under Federal Motor Carrier Safety Administration rules, drivers must renew the HME at least once every five years, although a State may require more frequent renewals.

Source: [http://www.tsa.gov/public/display?theme=44&content=090005198\\_013062d](http://www.tsa.gov/public/display?theme=44&content=090005198_013062d)

7. *June 01, USA TODAY* — **United, unions head off strike threat.** United Airlines averted the threat of a paralyzing strike Tuesday, May 31, when it reached an agreement in principle on a new contract with its largest union, the International Association of Machinists (IAM). In addition, a second union representing United's aircraft mechanics announced its members approved a new cost-cutting labor contract with the airline, the country's second-largest airline. United, which has been in bankruptcy reorganization 21/2 years, praised the developments, which are designed to cut costs as the airline struggles to exit bankruptcy. United has said for months it needs the cost cuts to attract \$2 billion or more in exit financing from lenders. The airline already has won additional cost cuts from its flight attendants and pilots. The deal with the IAM, if it is approved, would bring the total labor savings to \$700 million a year for five years. These events "move us significantly forward in our restructuring and set the stage for our exit from bankruptcy," United officials said. The mechanics union, which represents 7,000 United workers, said 59% of its voting members approved a new five-year contract that cuts pay 3.9% starting Wednesday, June 1. The contract will save United \$96 million a year.

Source: [http://www.usatoday.com/travel/news/2005-05-31-united-machinists\\_x.htm](http://www.usatoday.com/travel/news/2005-05-31-united-machinists_x.htm)

8. *May 31, CNN* — **Report: Costs, delays harm air traffic upgrade.** Sharp cost increases and delays in implementation are harming efforts to modernize the U.S. air traffic control system, the Department of Transportation's Office of Inspector General (IG) said in a report released Tuesday, May 31. At a time when air travel continues to grow, the Federal Aviation Administration (FAA) has become focused on maintaining the system it already has, rather than increasing capacity through system enhancements, said the report. Sixteen FAA projects — like new terminals for air traffic controllers and equipment to prevent runway accidents — were examined and 11 were found to have grown by over \$5.6 billion, pushing total current costs to about \$14.5 billion. Nine of the 16 projects had delays ranging from two to 12 years and two projects have been deferred. Congress appropriated \$2.5 billion for facilities and equipment funding for fiscal 2005 that ends September 30. The report said the FAA needed to reassess the benefits and timing of each project given the cost increases, the delays and cuts in congressional funding for equipment purchases.

Report: <http://www.oig.dot.gov/StreamFile?file=/data/pdffdocs/av2005061.pdf>

Source: <http://www.cnn.com/2005/TRAVEL/05/31/transport.faa.reut/index.html>

9. *May 31, Department of Transportation* — **Grant targets leading causes of rail-related deaths.** A \$1 million safety grant will be used for public education and outreach programs to reduce fatalities resulting from highway-rail grade crossing collisions, pedestrian accidents and railroad trespassing, which together account for 96 percent of all rail-related deaths, the Federal Railroad Administration (FRA) announced on Tuesday, May 31. The grant will fund various activities of Operation Lifesaver, Inc. (OLI) a not-for-profit organization that provides educational and awareness programs to inform motorists about how to safely approach highway-rail grade crossings, and to prevent individuals from trespassing on railroad property. Specifically, the funds will be used for programs in more than 40 states, training for nearly

5,000 volunteer presenters and expand OLI's ongoing national public service announcement campaign. Also, the OLI grant supports a major goal of the Department of Transportation's new National Rail Safety Action Plan to improve the awareness of the role motorists, railroads, states, and local communities each have in achieving grade crossing safety.

Source: <http://www.dot.gov/affairs/fra1105.htm>

[\[Return to top\]](#)

## **Postal and Shipping Sector**

Nothing to report.

[\[Return to top\]](#)

## **Agriculture Sector**

10. *June 01, Associated Press* — **Bird flu not behind chicken illness in Brazil.** Authorities have ruled out bird flu as the cause of a mysterious respiratory illness that prompted the slaughter of 17,000 chickens in a central western Brazilian state, an official with the Agriculture Ministry said Wednesday, June 1. "We know it's not bird flu," Jamil Gomes, coordinator of the ministry's animal sanitation division, said. "It has not arrived in South America." Testing was still under way to identify the disease, but Gomes said authorities suspect it may be Exotic Newcastle disease, which paralyzes and kills all species of birds. The slaughter was ordered last week at a farm in Mato Grosso do Sul state where 5,000 chickens had died, but officials did not make the news public until Tuesday, May 31, and initially refused to describe the symptoms that the chickens were suffering from. Brazil is the world's largest chicken exporter.

Source: [http://www.washingtonpost.com/wp-dyn/content/article/2005/06/01/AR2005060100714\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2005/06/01/AR2005060100714_pf.html)

11. *June 01, USAgNet* — **Canada finds bird flu strain on turkey farm.** The Canadian Food Inspection Agency has quarantined a turkey layer farm in Abbotsford, British Columbia, based on preliminary results from the British Columbia Ministry of Agriculture, Food and Fisheries, indicating the presence of the H3 influenza virus in the flock. The turkey farm is near a swine farm that recently experienced an H3 influenza infection and the virus is suspected to have originated from swine. This low pathogenic H3 virus is a milder form of virus and has not been known to mutate into high pathogenic avian influenza.

Source: <http://www.usagnet.com/story-national.cfm?Id=561&yr=2005>

12. *June 01, Greeley Tribune (CO)* — **Colorado State University leads animal-tracking project.** Colorado State University is piloting a national animal identification system that will rely on grid-computing technology to process massive amounts of animal tracking data. The project, the first to use Colorado State's new Colorado Grid Computing Initiative, or COGrid, is funded through more than two million dollars in grants from the Colorado Institute of Technology and additional funding and equipment from Sun Microsystems, the U.S. Department of Homeland Security, and the Colorado Department of Agriculture. The grid computing identification system will enable researchers to track the travels of a specific animal in seconds or minutes, instead of the weeks it currently takes. In case of a disease outbreak,

having a national database of cattle would allow officials to find out where a cow has been at all times from birth to death. Officials could identify all of the cow's co-residents for immediate testing, limiting the spread of the disease. Grid computing treats computational power as a utility, the same way that an electrical grid delivers electricity.

Source: [http://www.greeleytrib.com/article/20050601/BUSINESS/1060100\\_66](http://www.greeleytrib.com/article/20050601/BUSINESS/1060100_66)

13. *May 31, Agriculture Online* — **Interactive site helps predict head scab.** As this year's wheat crop enters the flowering stage, growers are being encouraged to stay on top of the latest predictions from the Fusarium Head Blight Prediction Center's early warning system. The system uses the flowering dates of wheat and weather data to predict the risk of head scab for wheat fields in 23 states. The system is a joint project between Ohio State University Extension, Penn State University, Purdue University, North Dakota State University, South Dakota State University, and the U.S. Wheat and Barley Scab Initiative.

Interactive tool: <http://www.wheatcab.psu.edu/riskTool.html>

Source: [http://www.agriculture.com/ag/story.jhtml?storyid=/templatedata/ag/story/data/agNews\\_050531crWHEAT.xml&catref=ag1001](http://www.agriculture.com/ag/story.jhtml?storyid=/templatedata/ag/story/data/agNews_050531crWHEAT.xml&catref=ag1001)

14. *May 31, Register-Guard (OR)* — **Unknown rust fungus arrives on Oregon coast.** State agriculture officials say that a species of rust fungus never before seen in North America has shown up along the southern Oregon Coast. The fungus strain, which will be confirmed through DNA analysis, has attacked some of the weedy Himalayan blackberry plants that infest the area. "What we know about the rust is that it is very specific and has a narrow host range," said Tim Butler, of the state Department of Agriculture. The rust appears to be confined to about 100 square miles of Coos and Curry counties. State officials say the rust probably is *Phragmidium violaceum*, which is used as a biological control agent for unwanted blackberry species in Australia, New Zealand, and Chile. It leaves purple spots on the top of the leaves of Himalayan blackberry — a non-native, aggressive species that is widespread in Western Oregon — with corresponding yellow pustules underneath the leaves. The rust reduces the plant's vigor and there can be some die-back of the cane. To learn more about the rust, the Department of Agriculture, the Oregon State University Extension Service and the federal Agricultural Research Service have set up a "trap garden" in a patch of infected Himalayan blackberry. There, commercial varieties of blackberry are intentionally planted to see if the rust also will attack them.

Source: [http://www.registerguard.com/news/2005/05/30/c1.cr.berryrust\\_0530.html](http://www.registerguard.com/news/2005/05/30/c1.cr.berryrust_0530.html)

[[Return to top](#)]

## **Food Sector**

15. *May 31, Bloomberg* — **Australia judge says U.S., Canada pork threatens domestic herds.** An Australian judge ruled that pork imported from the U.S. and other countries may lead to an outbreak of a deadly disease that affects young pigs, citing inadequacies in the nation's quarantine system. Judge Murray Wilcox ruled May 27 the present quarantine system may not stop post-weaning multisystemic wasting syndrome (PMWS) from attacking young pigs in Australia, one of the few nations without the disease. Importing the pork from infected countries such as Denmark, Canada, or the U.S. could expose Australia pigs, Wilcox ruled. "We didn't expect the judge to rule the risk assessment procedure was invalid," said Richard

Fritz, a vice president for the U.S. Meat Export Federation. The ruling "could impact exports immediately if importers or exporters fear the meat could get stuck" in transit if the ruling is affirmed, Fritz said. PMWS has become an increasing problem in recent years in Canada, the U.S., and Europe. The illness usually affects pigs after they reach six to eight weeks of age and mortality rates in infected herds can exceed 25 percent.

Source: <http://www.bloomberg.com/apps/news?pid=10000081&sid=aqv0FbMEUBss&refer=australia>

16. *May 31, Reuters* — **Korea veterinary experts to visit U.S.** South Korean veterinary experts will meet U.S. counterparts to discuss mad cow safeguards next week in a visit that may bring Seoul closer to ending a ban on U.S. beef. Beef shipments were cut off in December 2003 following the U.S. announcement of its first case of mad cow disease. South Korea was the third-largest market for U.S. beef. A South Korean newspaper said on Sunday, May 29, the June meeting, the third session between the countries, might conclude with a decision to end the ban on U.S. beef. Members of South Korean consumer groups visited U.S. farms, slaughterhouses and feed mills in early May to see preventive steps against mad cow disease. Source: <http://www.reuters.com/newsArticle.jhtml?type=politicsNews&storyID=8655717>

[[Return to top](#)]

## **Water Sector**

Nothing to report.

[[Return to top](#)]

## **Public Health Sector**

17. *June 01, Journal of the American Medical Association* — **Access to trauma centers in the U.S.** Previous studies have reported that the number and distribution of trauma centers are uneven across states, suggesting large differences in access to trauma center care. Researchers estimated the proportion of U.S. residents having access to trauma centers within 45 and 60 minutes. A cross-sectional study was done using data from two national databases. Trauma centers, base helipads, and block group population were counted for all 50 states and the District of Columbia as of January 2005. An estimated 69.2 percent and 84.1 percent of all U.S. residents had access to a level I or II trauma center within 45 and 60 minutes, respectively. The 46.7 million Americans who had no access within an hour lived mostly in rural areas, whereas the 42.8 million Americans who had access to 20 or more level I or II trauma centers within an hour lived mostly in urban areas. Within 45 and 60 minutes, respectively, 26.7 percent and 27.7 percent of U.S. residents had access to level I or II trauma centers by helicopter only and 1.9 percent and 3.1 percent of U.S. residents had access to level I or II centers only from trauma centers or base helipads outside their home states. Source: <http://jama.ama-assn.org/cgi/content/short/293/21/2626>

18. *May 31, Albuquerque Tribune (NM)* — **New Mexico devises plan for potential flu pandemic.** The plan probably will be in place by late summer, said State epidemiologist Mack Sewell. Some aspects of the state plan will be getting the first vaccines and protective equipment to

state health care workers and shutting down public places like schools and shopping malls. Efforts to find new types of vaccines — which would be the most effective tool — are in only the most primitive planning stages locally and globally, Sewell said. Sewell is president-elect of the national Council of State and Territorial Epidemiologists, which is working with the Centers for Disease Control and Prevention on a national pandemic preparedness plan. Bird flu turns into human flu when the disease spreads from birds to people. It can turn into a pandemic when the disease mutates in people so that it can be transmitted from person to person. "It is sobering to realize that when the last pandemic emerged in 1968 in China, the human population was 790 million and the poultry population was 12.3 million; today those numbers are 1.3 billion and 13 billion, respectively," said Michael Osterholm, director of the Center for Infectious Disease Research and Policy at the University of Minnesota. The larger populations mean even more chances for the disease to leap from birds to people.

Source: [http://www.abqtrib.com/albq/nw\\_science/article/0.2668.ALBO\\_21236\\_3819042.00.html](http://www.abqtrib.com/albq/nw_science/article/0.2668.ALBO_21236_3819042.00.html)

19. *May 31, Sci-Tech Today* — **World Health Organization: Marburg outbreak is under control.** A senior World Health Organization (WHO) official said Tuesday, May 31, authorities have brought under control Angola's Marburg virus outbreak, though the epidemic is not yet close to eradication. The outbreak that has killed 334 people "is under control. At the moment, the epidemic's peak has passed and the trend is very favorable," Luis Gomes Sambo, the WHO Regional Director for Africa, told reporters. However, the incubation period for the virus can be 21 days. WHO officials have said they do not consider outbreaks to be contained until there have been no new infections for double the maximum incubation time. The WHO said last week the number of infections is tailing off, but new cases are still emerging and any one of them could spark a new crisis.

Source: [http://www.sci-tech-today.com/story.xhtml?story\\_id=35837](http://www.sci-tech-today.com/story.xhtml?story_id=35837)

[\[Return to top\]](#)

## **Government Sector**

Nothing to report.

[\[Return to top\]](#)

## **Emergency Services Sector**

20. *June 01, Associated Press* — **Mississippi improves hurricane evacuation routes.** The Mississippi Emergency Management Agency (MEMA) is changing some evacuation procedures this year to try to prevent bottlenecks like the ones that occurred in and around Hattiesburg before Hurricane Ivan. Hurricane season officially begins on Wednesday, June 1. MEMA officials say local law-enforcement officials will be allowed to manually control traffic lights to speed up traffic on U.S. 49, the main route between Gulfport and Jackson, MS. Motorists traveling north from the coastal areas of Mississippi, Alabama, and Louisiana complained of being stuck for hours around Hattiesburg near the interchanges between U.S. 49 and U.S. 98, and between U.S. 49 and Interstate 59, one of the main routes out of New Orleans. Governor Haley Barbour appointed Commissioner of Public Safety George Phillips to lead a

commission that studied the response to Ivan, which threatened Mississippi before walloping Alabama and Florida. "We realized the traffic signals along U.S. 49 were causing the greatest delays in Gulfport, Hattiesburg and south of Jackson, and that had to be addressed before this season," Phillips said.

Source: <http://www.picayuneitem.com/articles/2005/06/01/news/10evacu ation.txt>

**21. *June 01, Mount Vernon News (OH)* — Communication key in Ohio disaster drill.**

Communication was a key component in a mock disaster drill held Thursday, May 26, near the old Bible college in Bangs, OH. Issues ranged from initial confusion as to where the Red Cross shelter was set up, to not all units being on the same radio frequency, to communication equipment used by the health department working well. The scenario for the drill was a chemical spill: The 9-1-1 dispatch center received a call from a farmer who noticed one of his anhydrous ammonia tanks had been removed from his farm. The Central Ohio Joint Fire District responded with a medic and truck. EMS personnel evaluated and triaged the victims; mutual aid was called for, with Mount Vernon, College and Delaware departments responding. Four members of the Citizen Emergency Response Team, a group formed through the Knox County Citizen Corps Council, were dispatched to direct traffic. The Knox County Sheriff's Office also responded to help with traffic control. The Ohio EPA was on scene, and personnel simulated checking nearby residences to see if anyone reported having any symptoms. The drill was evaluated by officials from the emergency management agencies in Delaware, Morrow and Holmes counties.

Source: <http://www.mountvernonnews.com/local/052705/drill.html>

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

**22. *May 31, SecurityFocus* — PHP multiple local and remote vulnerabilities.** PHP4 and PHP5 are reported prone to multiple local and remote vulnerabilities that may lead to code execution within the context of the vulnerable process. PHP safe\_mode\_exec\_dir is reported prone to an access control bypass vulnerability. A local attacker that can manipulate the directory name from which the PHP script is called, may bypass 'safe\_mode\_exec\_dir' restrictions by placing shell metacharacters and restricted commands into the directory name of the current directory. This may allow them to gain access to potentially sensitive information, such as database credentials. Refer to Source link below for vendor solutions.

Source: <http://www.securityfocus.com/bid/11964>

**23. *May 31, SecurityFocus* — MyBB multiple cross-site scripting and SQL injection vulnerabilities.** MyBB is prone to multiple cross-site scripting and SQL injection vulnerabilities. These issues are due to a failure in the application to properly sanitize user supplied input. The application is prone to multiple SQL injection vulnerabilities. Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation. Updates available at: <http://mybboard.com/community/attachment.php?aid=862>

Source: <http://www.securityfocus.com/bid/13827>

24. *May 31, SecurityFocus* — **Microsoft Windows Hyperlink Object Library buffer overflow vulnerability.** The Microsoft Windows Hyperlink Object Library is reported prone to a buffer overflow vulnerability. An attacker may exploit this condition to execute arbitrary code on a vulnerable computer, which may grant unauthorized access to the computer or lead to privilege escalation. It is reported that issue presents itself when a user follows a malformed link specially crafted by an attacker, however, other attack vectors also exist to exploit this vulnerability. Specifically, an application that employs the affected library by accepting and supplying parameters to the library may allow an attacker to exploit this vulnerability remotely and without user interaction. Updates available through Source link below.  
Source: <http://www.securityfocus.com/bid/12479>

25. *May 31, ZDNet News* — **FBI and DHS object to cell phones on airplanes.** The FBI and Department of Homeland Security (DHS) are objecting to a proposal to permit the use of cellular telephones and other wireless devices on airplanes. Unless telecommunications providers follow a lengthy list of eavesdropping requirements for calls made aloft, the FBI and DHS don't want cellular or wireless connections to be permitted. In a letter to the Federal Communications Commission (FCC) sent last Thursday, May 26, the police agencies said any rule permitting "in-flight personal wireless telephone use must consider public safety and national security" concerns. At the moment, technical and social reasons keep cell phones muted during flight. The FCC is considering proposals to relax those restrictions. The FBI and DHS say that the 1994 Communications Assistance for Law Enforcement Act, or CALEA, requires that airlines follow strict wiretapping guidelines. The police agencies, for instance, want to be able to eavesdrop on conversations no "more than 10 minutes" after the call is made. "There is a short window of opportunity in which action can be taken to thwart ... crisis situations onboard an aircraft, and law enforcement needs to maximize its ability to respond to these potentially lethal situations," the agencies say in their letter.  
Letter to FCC: [http://www.askcalea.com/docs/20050526\\_doj\\_fcc-wt-04-435.pdf](http://www.askcalea.com/docs/20050526_doj_fcc-wt-04-435.pdf)  
Source: [http://news.zdnet.com/2100-1035\\_22-5726850.html](http://news.zdnet.com/2100-1035_22-5726850.html)

## Internet Alert Dashboard

### DHS/US-CERT Watch Synopsis

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US-CERT Operations Center Synopsis:** US-CERT reports a heap-based buffer overflow that affects the PHP 'pack()' function call. An attacker that has the ability to make the PHP interpreter run a malicious script may exploit this condition to execute arbitrary instructions in the context of the vulnerable process. This function allows a malicious programmer to set references to entries of a variable hash that have already been freed. This can lead to remote memory corruption and may allow them to gain access to potentially sensitive information, such as database credentials.

### Current Port Attacks

Top 10 Target Ports

135 (epmap), 445 (microsoft-ds), 1026 (----), 1027 (icq), 1433 (ms-sql-s), 1434 (ms-sql-m), 4899 (radmin), 139 (netbios-ssn), 1028 (----), 25 (smtp)

Source: <http://isc.incidents.org/top10.html>; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

## **Commercial Facilities/Real Estate, Monument & Icons Sector**

Nothing to report.

[\[Return to top\]](#)

## **General Sector**

Nothing to report.

[\[Return to top\]](#)

### **DHS/IAIP Products & Contact Information**

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

[DHS/IAIP Daily Open Source Infrastructure Reports](#) – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

[Homeland Security Advisories and Information Bulletins](#) – DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: <http://www.dhs.gov/dhspublic/display?theme=70>

### **DHS/IAIP Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS/IAIP Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS/IAIP Daily Report Team at (703) 983-3644 for more information.

### **Contact DHS/IAIP**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **DHS/IAIP Disclaimer**

The DHS/IAIP Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.